**UNITED STATES DISTRICT COURT**
**FOR THE EASTERN DISTRICT OF MICHIGAN**
**SOUTHERN DIVISION**

---

ROYAL TRUCK & TRAILER SALES
AND SERVICE, INC.,

Plaintiff,

v. No. 18-10986

MIKE KRAFT AND KELLY MATTHEWS,

Defendants.
_____ /

**OPINION AND ORDER GRANTING DEFENDANTS' MOTION TO DISMISS, DISMISSING WITHOUT PREJUDICE PLAINTIFF'S REMAINING STATE CLAIMS, AND DENYING AS MOOT DEFENDANTS' MOTION TO STAY DISCOVERY**

Plaintiff Royal Truck & Trailer Sales and Service, Inc. ("Royal Truck") brings claim against two of its former employees, Defendants Mike Kraft and Kelly Matthews, based on Defendants' alleged misappropriation of Plaintiff's company information prior to Defendants resigning from the company. Pending before the court are two motions filed by Defendants: a motion to dismiss (Dkt. #11) and a motion to stay discovery (Dkt. #18.) These motions have been fully briefed, and the court concludes that a hearing is not necessary. *See* E.D. Mich. 7.1(f)(2). For the reasons stated below, the court will grant Defendants' motion to dismiss, dismiss without prejudice Plaintiff's remaining state law claims, and deny as moot Defendants' motion to stay.

## I. BACKGROUND

Plaintiff is a Michigan-based truck supply and service company. Both Defendants are former employees of Plaintiff who accepted employment at a competitor of Plaintiff shortly after their resignations. While working for the company, both Defendants received company laptops, cell phones, and email addresses and were permitted to

access Plaintiff's customer and employee information. Defendants' access to this information, Plaintiff asserts, was limited by policies described in the Plaintiff's employee handbook. This handbook included an "Information Security/Confidentiality" policy which prohibited employees from using company information for nonbusiness purposes and sharing proprietary information with competitors. Plaintiff alleges that Defendants were familiar with these policies.

According to Plaintiff, Defendants exceeded their authorized access to their company-provided cellphones, laptops, and email accounts by accessing and using information in violation of Plaintiff's information policies. Plaintiff specifically alleges that before resigning, Defendants forwarded customer quotes, employee paystubs, and confidential sales figures to their personal email accounts and erased information and programs from their company devices. Based on these actions, Plaintiff brings claim for violation of the Computer Fraud and Abuse Act ("CFAA") as well as state law claims for conversion, breach of the duty of loyalty, tortious inference with a business relationship, and civil conspiracy.

Defendants do not explicitly deny these allegations but rather argue that Plaintiff's allegations do not form a cognizable claim under the CFAA.[1]

## II. STANDARD

Federal Rule of Civil Procedure 12(b)(6) provides for dismissal of a complaint for failure to state a claim upon which relief may be granted. Under the Rule, the court

[1] The court notes that Defendants failed to include a statement regarding Defendants' attempt to seek concurrence as required by Local Rule 7.1(a) in either of their motions. E.D. Mich. LR 7.1(a). Plaintiff's lack of concurrence to these motions is presumed based on Plaintiff's responses. Nevertheless, the court cautions that failure to comply with the court's Local Rules can result in motions being stricken without consideration.

construes the complaint in the light most favorable to the plaintiff and accepts all well-pleaded factual allegations as true. *Barber v. Miller*, 809 F.3d 840, 843 (6th Cir. 2015).

Federal Rule of Civil Procedure 8 requires a plaintiff to present in her complaint "a short and plain statement of the claim showing that the pleader is entitled to relief." A complaint must provide sufficient facts to "state a claim to relief that is plausible on its face." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that defendant acted unlawfully." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Twombly*, 550 U.S. at 556). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Id.* (citing *Twombly*, 550 U.S. at 555).

"A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678 (citing *Twombly*, 550 U.S. at 555). "To state a valid claim, a complaint must contain either direct or inferential allegations respecting all the material elements to sustain recovery under some viable legal theory." *Boland v. Holder*, 682 F.3d 531, 534 (6th Cir. 2012) (emphasis removed) (citing *League of United Latin Am. Citizens v. Bredesen*, 500 F.3d 523, 527 (6th Cir. 2007)). Determining whether a complaint states a plausible claim for relief is "a context-specific task that requires the reviewing court to draw on its judicial experience and common sense." *Iqbal*, 556 U.S. at 678 (citing *Twombly*, 550 U.S. at 555).

## III. DISCUSSION

Defendants' motion to dismiss raises a narrow issue, which currently forms a circuit split: whether the Computer Fraud and Abuse Act ("CFAA") governs situations in which employees who are authorized to access their employer's information use that information in violation of their employer's policies. For the reasons explained below, the court finds that it does not and, therefore, the court will grant Defendants' motion to dismiss.

### A. CFAA Claims

The CFAA is criminal, anti-hacking statute that also creates a private cause of action for "[a]ny person who suffers damage or loss by reason of a violation of this section[.]" 18 U.S.C. § 1030(g). The portion of the statute at issue in this case prohibits individuals from knowingly accessing a protected computer "without authorization" or in a manner that "exceeds authorized access." 18 U.S.C. § 1030(a)(2). To state a claim, Plaintiff must prove that Defendants "(1) accessed a protected computer; (2) without authorization or exceeded authorized access; and (3) there was damage or loss to plaintiff of more than $5,000 of value in a one-year period." *Senderra Rx Partners, Ltd. Liab. Co. v. Loftin*, No. 15-13761, 2016 U.S. Dist. LEXIS 173203, at *6 (E.D. Mich. Dec. 8, 2016). Defendants' motion to dismiss challenges Plaintiff's ability to satisfy the second element. Here, Plaintiff alleges that Defendants exceeded their "authorized access" in forwarding price quotes, employee pay stubs, and sales information to their personal email accounts in violation of company policies. Courts are not in universal agreement as to whether an employee's violation of company policies implicates the CFAA.

In *Ajuba Int'l, L.L.C. v. Saharia*, 871 F. Supp. 2d 671 (E.D. Mich. 2012) (Battani, J.), the court aptly summarizes the two approaches taken by courts that have analyzed the CFAA's "exceeds authorized access" language:

> Some courts have construed the terms narrowly, holding that an employee's misuse or misappropriation of an employer's business information is not "without authorization" so long as the employer has given the employee permission to access such information. *See LVRC Holdings L.L.C. v. Brekka*, 581 F.3d 1127 (9th Cir. 2009) (holding that that the CFAA targets the unauthorized procurement or alteration of information rather than its misuse); *Orbit One Commc'ns, Inc. v. Numerex Corp*., 692 F.Supp.2d 373, 385 (S.D. N.Y. 2010) ("The plain language of the CFAA supports a narrow reading. The CFAA expressly prohibits improper 'access' of computer information. It does not prohibit misuse or misappropriation."). . . In other words, courts adopting the narrow approach hold that, once an employee is granted "authorization" to access an employer's computer that stores confidential company data, that employee does not violate the CFAA regardless of how he subsequently uses the information.
>
> Other courts have construed the terms broadly, finding that the CFAA covers violations of an employer's computer use restrictions or a breach of the duty of loyalty under the agency doctrine. *See United States v. Rodriguez*, 628 F.3d 1258(11th Cir. 2010); *United States v. John*, 597 F.3d 263 (5th Cir. 2010); *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006); *EF Cultural Travel BV v. Explorica, Inc*., 274 F.3d 577 (1st Cir. 2001). The broad approach holds that "an employee accesses a computer 'without authorization' whenever the employee, without the employer's knowledge, acquires an interest that is adverse to that of his employer or is guilty of a serious breach of loyalty." *Guest-Tek Interactive Entm't, Inc. v. Pullen*, 665 F.Supp.2d 42, 45 (D. Mass. 2009).

*Id*. at 686–87.

The Sixth Circuit has not directly considered this issue. *Id*. at 686. However, two of three of courts in this district to address this issue have adopted the narrow approach. *See Senderra Rx Partners, Ltd. Liab. Co. v. Loftin*, No. 15-13761, 2016 U.S. Dist. LEXIS 173203, at *6 (E.D. Mich. Dec. 8, 2016) (Cohn, J.); *see contra Am. Furukawa, Inc. v. Hossain*, 103 F. Supp. 3d 864, 876 (E.D. Mich. 2015) (Drain, J.). Additionally, the majority of district courts in the Sixth Circuit to address this issue have

adopted the narrow approach. *See Experian Mktg. Sols., Inc. v. Lehman*, No. 15-CV-476, 2015 WL 5714541, at *5 (W.D. Mich. Sept. 29, 2015) (Bell, J.); *Cranel Inc. v. Pro Image Consultants Grp., LLC*, 57 F. Supp. 3d 838, 845 (S.D. Ohio 2014) (Graham, J.); *Dana Ltd. v. Am. Axle & Mfg. Holdings, Inc*., No. 10-CV-450, 2012 WL 2524008, *5 (W.D. Mich. June 29, 2012) (Bell, J.); *ReMedPar, Inc. v. AllParts Med., L.L.C.*, 683 F. Supp. 2d 605, 609 (M.D. Tenn. 2010) (Wiseman, Jr., J.); *Black & Decker, Inc. v. Smith*, 568 F. Supp. 2d 929 (W.D. Tenn. 2008) (Breen, J.); *Am. Family Mut. Ins. Co. v. Rickman*, 554 F.Supp.2d 766, 771 (N.D. Ohio 2008) (Zouhary, J.).

With any issue of statutory interpretation, the court begins by analyzing the plain meaning of the statute. *See Perez v. Postal Police Officers Ass'n*, 736 F.3d 736, 741 (6th Cir. 2013). The court is persuaded that the plain meaning of the CFAA necessitates the adoption of the narrow approach. As explained by the Ninth Circuit Court of Appeals in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), the term "authorization" must be interpreted by its ordinary meaning because it is not defined in the statute. *Id*. at 1132. Authorization is defined as "permission or power granted by an authority." *Id*. (quoting *Authorization*, Random House Unabridged Dictionary, 139 (2001); *Authorization*, Webster's Third International Dictionary, 146 (2002)). The Ninth Circuit reasoned that this definition implies that "an employer gives an employee 'authorization' to access a company computer when the employer gives the employee permission to use it." Based on this plain meaning, when an employer allows an employee to access a computer, such as in this case, an employee does not act "without authorization" even if the employee uses the computer for a personal purpose. *See id*. Therefore, the statute's "without authorization" language does not apply to

situations, such as those alleged in the complaint, where the plaintiff authorized the defendant to access the information at issue.[2]

The court also echoes the concern raised by other courts that adopting the board approach and allowing employers to recover against employees for violating internal information polices would transform a criminal statute, initially intended to punish hackers, into a federal cause of action for a breach of the duty of loyalty. *See, e.g.*, *Am. Family Mut. Ins. Co. v. Rickman*, 554 F. Supp. 2d 766, 771 (N.D. Ohio 2008) ("The statute was not meant to cover the disloyal employee who walks off with confidential information. Rather, the statutory purpose is to punish trespassers and hackers.").

Plaintiff's CFAA claims are exclusively based on Defendants' alleged violation of company policy. (Dkt. 13, PageID 109.) The court's determination that the CFAA does not extend to such conduct, therefore, ends the court's inquiry into Plaintiff's CFAA claims.

**B. State Law Claims**

In the absence of any surviving claims under federal law, the court will decline to exercise supplemental jurisdiction over Plaintiff's remaining state law claims. *See Novak v. MetroHealth Med. Ctr.*, 503 F.3d 572, 583 (6th Cir. 2007) (citing 28 U.S.C. § 1367(c)(3)) ("A district court may decline to exercise supplemental jurisdiction over state

[2] At least some of the courts to favor the narrow approach also rely on "the rule of lenity and the statutory canon of avoiding absurd results" and "the legislative history and congressional intent" as supporting such a finding. *See, e.g.*, *Ajuba Int'l, L.L.C.*, 871 F. Supp. 2d at 687. Being mindful of "the thicket of legislative history," *United States v. Gonzales,* 520 U.S. 1, 4 (1997), the court merely notes these points in passing without adoption or analysis. *See id.* at 6 ("Given the straightforward statutory command, there is no reason to resort to legislative history.").

law claims if it has dismissed all claims over which it had original jurisdiction."). The court will dismiss without prejudice Plaintiff's remaining claims for conversion, breach of the duty of loyalty, tortious interference, and civil conspiracy.

## IV. CONCLUSION

The court is not persuaded that the CFAA applies to the misappropriation of information by employees authorized to access their company's data. Accordingly,

IT IS ORDERED that Defendants' motion to dismiss (Dkt. #11) is GRANTED. The court DECLINES to exercise supplemental jurisdiction over Plaintiff's remaining state claims and DISMISSES these claims WITHOUT PREJUDICE.

IT IS FURTHER ORDERED that Defendants' motion to stay discovery (Dkt. #18.) is DENIED AS MOOT.

s/Robert H. Cleland
ROBERT H. CLELAND
UNITED STATES DISTRICT JUDGE

Dated: March 11, 2019

I hereby certify that a copy of the foregoing document was mailed to counsel of record on this date, March 11, 2019, by electronic and/or ordinary mail.

s/Lisa Wagner
Case Manager and Deputy Clerk
(810) 292-6522

S:\Cleland\Cleland\HEK\Civil\18-10986.ROYAL.TRUCK.cfaa.mtd.HEK.2.RHC.3.docx